Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

SECOND PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)	
JRL-3995-42 Confirmation No. 4649	

Application Number	Filed
10/530,293	April 5, 2005
First Named Inventor	
NÄSLUND	
Art Unit	Examiner
2435	Schwartz, Darren B.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ Applicant/Inventor

☐ Assignee of record of the entire interest. See 37 C.F.R. § 3.71. Statement under 37 C.F.R. § 3.73(b) is enclosed. (Form PTO/SB/96)

☒ Attorney or agent of record 33,149 (Reg. No.)

☐ Attorney or agent acting under 37CFR 1.34.
Registration number if acting under 37 C.F.R. § 1,34 _____

Signature

John R. Lastova
Typed or printed name

703-816-4025
Requester's telephone number

January 10, 2011
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.*

☒ *Total of 1 form/s are submitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

NASLUND et al.

Atty. Ref.: 3995-42; Confirmation No. 4649

Appl. No. 10/530,293

TC/A.U. 2435

Filed: April 5, 2005

Examiner: Schwartz, Darren B.

For: SECURITY AND PRIVACY ENHANCEMENTS FOR SECURITY DEVICES

* * * * * * * * * * *

January 10, 2011

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SECOND PRE-APPEAL BRIEF REQUEST FOR REVIEW

Claims 44, 46, 49-59, 61, and 79-82 stand rejected under 35 USC §103(a) as being unpatentable based on a Wireless Identity Module protocol document referred to by the Examiner as WIM in view of newly-cited Takahashi and further in view of Aura (USP 6,711,400). This rejection is respectfully traversed.

WIM describes a tamper-resistant security device with a memory for storing user credentials like a security key and an AKA-module for performing AKA processing with the security key. WIM defines an interface between part of a WAP client device and the tamper-resistant security device, i.e., WIM defines an **external** interface to the security device. Page 63 of the WIM-document discloses a card (mapped to a tamper-resistant security device) incorporating a WIM-application and other applications so that these applications are protected and executed in a tamper-resistant environment. But there is no disclosure in WIM of an **internal** interface between the other applications or the WIM-application and the AKA-module. Input to and output from the WIM-application and the other applications are directed over the external interface to the tamper-resistant security device for processing by the WIM-application or other applications.

Nor does WIM disclose the claimed cooperating application or its post processing, as the Examiner agrees. The Examiner relies on Takahashi as allegedly teaching the cooperating

application and the claimed internal interface and on Aura as allegedly teaching the post processing. Applicants respectfully disagree.

The Examiner identifies Takahashi's point of deployment (POD) module 26 which can be an integrated circuit Smartcard that can be inserted into a slot or otherwise electrically coupled to a host device 24 corresponding to a set top box, a TV, VCR, or a PC. See col. 3, lines 12-22. The Examiner contends that Takahashi's POD module 26 corresponds to the claimed AKA module, the host 24 corresponds to the claimed cooperating application contained within a tamper-resistant security device (receiver 20), and that the "binding messages" sent by the external head-end system 14 and received at the receiver are used by the POD module 26 to determine if the host device 24 is an authorized device. If the host authentication is successfully based on the externally-provided binding information, then the POD module 26 transmits the externally-provided binding information to the host 24 and generates and stores a session key to use in protection of communications between the POD module 26 and the host device 24. See column 6, lines 22-29.

Takahashi's receiver 20 is not a tamper-resistant security device which as recited claim 44 contains the claimed AKA module, cooperating application, and application interface, e.g. claim 44 recites "a cooperating application, contained within the tamper-resistant security device" and "an application interface internal to the tamper-resistant security device." Given that the host 24 is an entire set top box, it is unreasonable to contend that it is a tamper-resistant security device. Indeed, this unreasonableness is evidenced by the explicit precautions that Takahashi acknowledges are needed for communications between the POD 26 and host 24 in the receiver 20. For example, Takahashi states: "To *protect information communicated between the POD module 26 and the host device 24*, a *copy or content protection* (CP) protocol may be implemented," col. 3, lines 19-21, and "a session key for *encrypting* and decrypting messages transmitted between the POD module 26 and host device 24," col. 3, lines 56-58 (emphasis added). But it would not be necessary to copy protect/encrypt the communications between the POD and host if the receiver 20 was a tamper-resistant security device.

Moreover, col. 3, lines 51-54 state that the POD and HOST must authenticate each other. Thus, not only is the receiver 20 assumed insecure in Takahashi with respect to eavesdropping, it is also assumed by Takahashi to be susceptible to tampering with the communication between the POD and HOST, e.g., in the form of impersonation. Accordingly, no one skilled in this art

would consider Takahashi's POD and HOST to be contained together in a same tamper-resistant security device.

Another evidence of this difference between Takahashi and the claimed tamper-resistant security device is found at col. 3, lines 12-22, where the POD is described as a smart card "being inserted into a slot of the host." In other words, the POD 26 and the host 24 are not part of the same tamper resistant device. Indeed, the POD could easily be removed after insertion and replaced by another "faked" POD. For this reason, it is also unreasonable to contend that the interface between POD 26 (mapped to the cooperating application) and the host 24 (mapped to the AKA module) corresponds to the claimed "internal" application interface contained with a tamper-resistant security device. The line connecting the POD and host cannot be internal since a user inserts and can remove the POD from the host slot.

In contrast to Takahashi, the technology in claim 44 places the cooperating application inside the same tamper resistant device in order to eliminate the need for the kind of explicit POD-HOST security mechanisms explicitly needed and disclosed in Takahashi. The claimed technology also simplifies the security procedures for a user/operator because moving the claimed tamper-resistant security device between different user devices (e.g., different mobile phones) automatically moves the cooperating application at the same time. But if the POD is moved between two hosts in Takashi, a user/operator needs to ensure that the new host (set top box) has the same cooperating application as the old host.

In addition to the multiple deficiencies already identified for WIM and Takahashi, the Examiner also admits that neither reference discloses or suggests that "said enhanced security processing by said cooperating application includes post-processing of at least one AKA output parameter produced by the AKA module in response to the one or more AKA process commands, said post-processing including encapsulation of said at least one AKA output parameter to generate a further AKA parameter that has higher security than said at least one AKA output parameter produced in response to the one or more AKA process commands," as recited in claim 44. The Examiner turns to a third reference to Aura and to a modified version of the GSM-based security procedures used for mobile phones shown in Figure 4.

Aura's mobile phone authentication method spans between a mobile station (MS), a visited public land mobile network (VPLMN), and an HLR/AUC node as shown in Figure 4. The Examiner contends that Aura's processing in the HLR/AUC node in block 405 and in the MS in block 407 corresponds to the claimed enhanced security processing. But the problem with

this reading is that Aura's enhanced security processing is performed in physically separate and remote nodes HLR/AUC and MS and occurs outside of a tamper-resistant security device, (which is the SIM card in the MS), rather than "contained within the tamper-resistant security device," as claimed. In fact, Aura's enhanced processing occurs across an entire visiting network VPLM as shown in Figure 4. This is the antithesis of a tamper-resistant security device used in a user device like the MS.

Another problem with Aura is that neither block 405 nor 407 can be the claimed cooperating application because neither cooperates with an existing AKA module nor operates on outputs of the AKA module. Both blocks 405 and 407 are the AKA modules in the HLR/AUC and MS, respectively. Unlike what is claimed, Aura's teachings are directed to replacing the normal GSM AKA module with a different, replacement AKA module. Specifically, Aura simply replaces the two A3 and A8 functions with three H1, H2, and H3 functions as is shown in blocks 405 and 407. This can be seen by comparing Figs. 3 and 4 side-by-side which makes it is clear that the A3 and A8 AKA functions of Fig. 3 are replaced by the H-functions of Fig. 4.

Moreover, to compute H1-H3 at the MS, Aura's MS needs direct access to the key Ki, which means that the AKA module 407 must already contain the key Ki as indicated in 407. This is necessary to ensure that the key Ki is not exposed outside of the AKA module for security reasons. Hence, the computations of H1-H3 are not "post-processing of at least one AKA output parameter." It is already established that 405 and 407 are not in the same security device. Each of Aura's blocks 405 and 407 performs a new AKA processing altogether operating on the inputs each of these blocks receive. To suggest that the claimed post-processing can be performed by another node across a network is the same as post-processing performed within the same security device is untenable and unreasonable.

Since the block 405 is the AKA module in Aura, it is unclear what in the HLR/AUC is performing the claimed post-processing since there is no other block that follows block 405 at the HLR/AUC in Fig. 4. If RAND2, SRES1, SRES2', and Kc are the AKA output parameters, Aura's HLR/AUC does not "generate a further AKA parameter that has higher security than said at least one AKA output parameter."

If the pre-appeal board maintains the final rejection, it is requested that they specifically identify what specific structure or feature in Aura corresponds to the claimed: (1) AKA module, (2) cooperating application, (3) received AKA process command(s), (4) enhanced AKA process

command(s), (5) post-processing operation, (6) encapsulation, (7) AKA output parameter, and (8) further AKA parameter because the column/line references in the final action are ambiguous and unclear.

The Examiner uses three references but never explains how the alleged GSM authentication between HLR and MS in Aura will be used specifically in Takahashi and WIM. For example, how are the commands from Aura's AKA module(s) Ki, RAND1/2, SRES1 and SRES1' to be used in Takahashi's POD 26? The difficulty in understanding how these three references would actually be used together underscores the impermissible hindsight nature of the rejection.

Several dependent claim features are also not taught by the three reference combination. For example, WIM section 11.3.6.4 simply describes a perform security operation command that "implements all security related APDU commands." It is not seen how this teaches "transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure," as recited in claim 56.

For claims 60 and 62, the Examiner relies on a fourth reference further evidencing the strained and improper hindsight attempt to reconstruct these claims in the final rejection.

The final rejection should be withdrawn and the case allowed.

Respectfully submitted,
NIXON & VANDERHYE P.C.

By: _____
John R. Lastova
Reg. No. 33,149

901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000